WHAT IS CLAIMED IS:

1.   A computer-implemented method for disabling on-demand resources on a computerized apparatus, comprising:

      receiving a disablement code;

      validating the disablement code; and

      disabling at least one on-demand resource.

2.   The computer-implemented method of claim 1 wherein validating comprises encrypting and decrypting data.

3.   The computer-implemented method of claim 1 wherein validating comprises verifying that the disablement code is unique to the at least one on-demand resource.

4.   The computer-implemented method of claim 1 wherein the at least one on-demand resource was previously enabled to allow a user to request usage of the at least one on-demand resource.

5.   The computer-implemented method of claim 1 wherein prior to disabling, the at least one on-demand resource is enabled to allow a user to request usage of the at least one on-demand resource; and wherein disabling the at least one on-demand resource comprises preventing the user from requesting usage of the at least one on-demand resource.

6.   The computer-implemented method of claim 1 wherein the at least one on-demand resource is a processor.

7.   The computer-implemented method of claim 1 wherein the at least one on-demand resource comprises one of memory and storage.

8.   The computer-implemented method of claim 1 wherein the disablement code is input by a user.

9.   A computer-implemented method for disabling on-demand resources on a computerized apparatus, comprising:

receiving a disablement code comprising encrypted data;

validating the disablement code, the validating comprising:

generating a first key using system information unique to the computerized apparatus;

decrypting the encrypted data using a second key to produce decrypted data;

encrypting a value to produce an encrypted value;

decrypting the encrypted value to produce a decrypted value; and

comparing the value to the decrypted value; and

disabling at least one on-demand resource if the validating is successful.

10.   The computer-implemented method of claim 9 wherein the validating is successful if the value and the decrypted value are the same.

11.   The computer-implemented method of claim 9 wherein the decrypted data is identical to the first key.

12.   The computer-implemented method of claim 9 wherein decrypting the encrypted data is performed by a smart chip containing the second key.

13.   The computer-implemented method of claim 9 wherein the at least one on-demand resource was previously enabled to allow a user to request usage of the at least one on-demand resource.

14.   The computer-implemented method of claim 9 wherein, prior to the disabling, the at least one on-demand resource is enabled to allow a user to request usage of the at least one on-demand resource and wherein disabling comprises preventing the user from requesting usage of the at least one on-demand resource.

15.   The computer-implemented method of claim 9 wherein the at least one on-demand resource is a processor.

16.   The computer-implemented method of claim 9 wherein the at least one on-demand resource comprises one of memory and storage.

17.   The computer-implemented method of claim 9 wherein the disablement code is input by a user.

18.   The computer-implemented method of claim 9 wherein encrypting the value to produce the encrypted value is done using an encryption key selected from one of (i) the decrypted data; and (ii) the first key.

19.   The computer-implemented method of claim 18 wherein decrypting the encrypted value to produce the decrypted value is done using (i) the first key if the value was encrypted using the decrypted data as the encryption key; and (ii) the decrypted data if the value was encrypted using the first key as the encryption key.

20.   A computer-implemented method for controlling availability of on-demand resources on a computerized apparatus, comprising:

      receiving an enablement code for an on-demand resource;

      validating the enablement code;

      enabling the on-demand resource, whereby usage of the on-demand resource may be requested by a user;

      receiving a disablement code for an on-demand resource;

validating the disablement code; and

disabling the on-demand resource; whereby usage of the on-demand resource may no longer be requested by the user.

21.   The computer-implemented method of claim 20 wherein validating the enablement code and validating the disablement code are performed by the same algorithm.

22.   The computer-implemented method of claim 20 wherein enabling comprises unlocking the on-demand resource.

23.   The computer-implemented method of claim 20 wherein the on-demand resource is computer hardware.

24.   The computer-implemented method of claim 20 wherein the on-demand resource is selected from one of processors, memory and storage.

25.   The computer-implemented method of claim 20 wherein validating the disablement code comprises verifying that the disablement code is unique to the on-demand resource.

26.   The computer-implemented method of claim 20 wherein the validating comprises:

generating a first key using system information unique to the computerized apparatus;

decrypting the encrypted data using a second key to produce decrypted data;

encrypting a value, using the first key as an encryption key, to produce an encrypted value;

decrypting the encrypted value, using the decrypted data as a decryption key, to produce a decrypted value; and

comparing the value to the decrypted value.

27. The computer-implemented method of claim 20 wherein the validating comprises:

generating a first key using system information unique to the computerized apparatus;

decrypting the encrypted data using a second key to produce decrypted data;

encrypting a value, using the decrypted data as an encryption key, to produce an encrypted value;

decrypting the encrypted value, using the first key, to produce a decrypted value; and

comparing the value to the decrypted value.

28. The computer-implemented method of claim 27 wherein the decrypted data is identical to the first key.

29. The computer-implemented method of claim 27 wherein the decrypting is performed by a smart chip containing the second key.

30. The computer-implemented method of claim 27 wherein the encrypted data was encrypted using a copy of the second key at a remote location.

31. A computer-implemented method for generating disablement codes for disabling on-demand resources on a computerized apparatus, comprising:

inputting a plurality of inputs to an authentication code generator, the plurality of inputs comprising machine identification information uniquely identifying the computerized apparatus;

outputting an authentication code;

encrypting the authentication code; and

providing a disablement code to a user of the computerized apparatus, the disablement code comprising the encrypted authentication code and being configured to disable an on-demand resource on the computerized apparatus upon being validated.

32. The computer-implemented method of claim 31, further comprising selling the computerized apparatus to the user.

33. The computer-implemented method of claim 31, further comprising providing the computerized apparatus to the user with an installed instance of the authentication code generator.

34. The computer-implemented method of claim 31, further comprising providing the computerized apparatus to the user with an installed instance of the authentication code generator and a smart chip containing a unique key used to perform the encrypting of the authentication code.

35. The computer-implemented method of claim 31, wherein encrypting the authentication code is performed using a unique key stored in a secure storage element on the computerized apparatus, the secure storage element being inaccessible to a user of the computerized apparatus.

36. A computer readable medium containing a program which, when executed, performs an operation for generating disablement codes for disabling on-demand resources on a computerized apparatus, the operation comprising:

receiving a plurality of inputs to an authentication code generator, the plurality of inputs comprising machine identification information uniquely identifying the computerized apparatus;

outputting an authentication code;

encrypting the authentication code; and

24

outputting a disablement code for the computerized apparatus, the disablement code comprising the encrypted authentication code and being uniquely configured to disable an on-demand resource on the computerized apparatus upon being validated.

37.   The computer readable medium of claim 36, wherein encrypting the authentication code is performed using a unique key stored in a secure storage element on the computerized apparatus, the secure storage element being inaccessible to a user of the computerized apparatus.

38.   A computer readable medium containing a program which, when executed, performs an operation for validating a disablement code for disabling on-demand resources on a computerized apparatus, the operation comprising:

receiving the disablement code comprising encrypted data; and

validating the disablement code, the validating comprising:

generating a first key using system information unique to the computerized apparatus;

sending the encrypted data to a secure storage element containing a second key, wherein the secure storage element is configured to decrypt the encrypted data, to produce decrypted data, using the second key;

generating a random value;

encrypting the random value using the first key to produce an encrypted random value;

sending the encrypted random value to the secure storage element, wherein the secure storage element is configured to decrypt the encrypted random value, using the decrypted data as decryption key, to produce a decrypted random value;

receiving the decrypted random value from the secure storage element; and

comparing the value to the decrypted random value.

39.   The computer readable medium of claim 38, wherein the first key is identical to the decrypted data.

40.   The computer readable medium of claim 38, wherein the secure storage element is a smart chip.

41.   The computer readable medium of claim 38, wherein the on-demand resource was previously enabled to allow a user to request usage of the on-demand resource.

42.   The computer readable medium of claim 38, further comprising disabling the on-demand resource, wherein the on-demand resource was previously enabled to allow a user to request usage of the on-demand resource and wherein disabling comprises preventing the user from requesting usage of the on-demand resource.

43.   The computer-implemented method of claim 38 wherein the on-demand resource is a processor.

44.   The computer-implemented method of claim 38 wherein the on-demand resource comprises one of memory and storage.

45.   The computer-implemented method of claim 38 wherein the disablement code is input by a user.

46.   A computer readable medium containing a program which, when executed, performs an operation for validating a disablement code for disabling on-demand resources on a computerized apparatus, the operation comprising:
    receiving the disablement code comprising encrypted data; and
    validating the disablement code, the validating comprising:
        generating a first key using system information unique to the
    computerized apparatus;

26

sending the encrypted data to a secure storage element containing a second key, wherein the secure storage element is configured to decrypt the encrypted data, to produce decrypted data, using the second key and further configured to encrypt a value using the decrypted data as an encryption key;

receiving the encrypted value from the secure storage element; and

decrypting the encrypted value using the first key.

47.   A computerized apparatus, comprising:

a plurality of resources at least one of which comprises an on-demand resource configured to be requested by a user once enabled; and

a capacity manager configured to at least:

receive an enablement code for the on-demand resource;

enable the on-demand resource;

receive a disablement code for the on-demand resource;

validate the disablement code; and

disable the on-demand resource.

48.   The computerized apparatus of claim 47, wherein the capacity manager is configured to validate the disablement code by encrypting and decrypting data.

49.   The computerized apparatus of claim 47, wherein the capacity manager is configured to validate by verifying that the disablement code is unique to the on-demand resource.

50.   The computerized apparatus of claim 47, wherein the on-demand resource comprises at least one of a processor, storage and memory.

51.   The computerized apparatus of claim 47, wherein the capacity manager configured to enable by unlocking the on-demand resource and making the on-demand resource available for use upon request.

52.   The computerized apparatus of claim 47, further comprising a user interface and wherein the capacity manager further configured receive the enablement code and disablement code from the user.

53.   The computerized apparatus of claim 47, wherein the capacity manager comprises a smart chip having an associated unique key.